UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,634	05/08/2006	Se Hyun Lee	035967-023	1419

46188 7590 11/13/2007

THELEN REID BROWN RAYSMAN & STEINER LLP
P. O. BOX 640640
SAN JOSE, CA 95164-0640

EXAMINER	
RUIZ, ANGELICA	

ART UNIT	PAPER NUMBER
2169	

MAIL DATE	DELIVERY MODE
11/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/578,634	LEE ET AL.	
	Examiner	Art Unit	
	Angelica Ruiz	2169	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 October 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *Jun/30/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-4 are rejected.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 10-2003-0080752, Country Rep. Of Korea, filed on November/14/2003.

Specification

3. The abstract of the disclosure is objected to because is not in the proper format. Correction is required. See MPEP § 608.01(b).

Applicant is reminded that ABSTRACT OF THE DISCLOSURE: See 37 CFR 1.72(b) and MPEP §608.01(b). A brief narrative of the disclosure as a whole in a single paragraph of 150 words or less commencing on a separate sheet following the claims. Further, in an international application which has entered the national stage (37 CFR 1.491(b)), the applicant need not submit an abstract commencing on a separate sheet if an abstract was published with the international application under PCT Article 21. The abstract that appears on the cover page of the pamphlet published by the International Bureau (IB) of the World Intellectual Property Organization (WIPO) is the abstract that will be used by the USPTO. See MPEP § 1893.03(e).

Claim Objections

4. Claims 1-4 are objected to because of the following informalities: Complete meaning for abbreviations: "AA, ACL, and ACE" should be stated and the abbreviation should be between parenthesis. Appropriate correction is required.

5. Claim 1 recites "server 300", numerical value is not permitted in the claimed language.

6. Claim 1 recites "this cookie". This pronoun only what is referred by "this" should set forth in the claim. To be consistent "cookie signal" should be replaced as "cookies information".

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-4 are rejected under 35 U.S.C. 102(b) as being anticipated by **Teng et al. (US Application No. 2002/0138577 A1).**

As per Claim 1, Teng discloses:

- An apparatus for managing access for an extranet, comprising:

(Abstract and Claim 30, "An **apparatus** according to claim 24, wherein: said one or more processors are part of an **integrated identity and access system**.") and (Par [0144], lines 7-11, "**Extranet and grant Extranet access** to many different companies. The entity setting up the Extranet is node 230. Each of the companies with Extranet access would have a node at a level below node 230.")

- **a plurality of domain web server, to which a plurality of users are subscribed,**

(Par [0479], "An Internet domain can reside on a single Web Server, or be distributed across multiple Web Servers. In addition, multiple Internet domains can reside on a single Web Server, or can be distributed across multiple Web Servers. In accordance with the present invention, the **Access System allows a user to satisfy the**

authentication requirements of a **plurality of domains** and/or Web Servers by performing a single authentication.") and (Par [0113], lines 1-8, "With **Group Manager 44,** companies (or other entities) can allow individual **users** to do the following: (1) self-**subscribe to and unsubscribe from groups**, (2) view the groups that they are eligible to join or have joined, and (3) request subscription to groups that have access to the applications they need. Multi-step workflows can then define which users must obtain approval before being added to a group and which can be added instantly.").

- **an AA server for managing access authentication and authorization for the domain web server,**

(Par [0109], lines 16-19, "An administrator can be delegated any allowed degree of responsibility. For example, a company might decide that only IT staff can assign **application access**") and (Par [0161], lines 1-7, "Configure tab 416 allows a user to configure various options for **User Manger 42**. The user must have sufficient privileges to access Configure tab 416. The user can perform attribute **access control**, delegate administration, define workflows and set the search base. **Attribute access control** includes controlling who has view and modify permissions for each attribute.").

- **an authority information storing module, and a user web browser interconnected with the AA server and the domain web server, wherein the AA server comprises an AA module playing a role of authentication and authorization;**

(Par [0398], lines 1-12, "If a status check is not required, **Identity Server** 40 exports the requested certificate to the user **via Web Server 20** (step 3434). ... Certificate Authority

2084, as described above with reference to FIG. 59A. In some embodiments, Identity Server 40 also **stores** the retrieved real time certificate status and related **validation information**") and (Par [0161], lines 5-7, "**Attribute access control** includes controlling who has view and modify permissions for each attribute.").

- **an ACL cache control module for synchronizing ACL caches of the respective domain web server with the AA server;**

(Par [0352], lines 2-13, "servers that are equipped to communicate with each other in accordance with the present invention. Identity Server 1900 contains a **set of function modules** 1904. Each function module contains instructions for carrying out a program that may be called for by a request. Function module set 1904 communicates with a set of caches 1906. Caches in set 1906 contain data frequently used by function modules in set 1904. **The following caches are representative of those in set 1906**: (1) **Access Control** Policy Cache; (2) System Specific Data Cache; (3) Workflow Definition Cache; (4) X Structure Cache; (5) Server Information Cache; (6) **Application Information Cache**; and (7) Master Audit Policy Cache.").

- **an encryption module for encrypting AA cookies to be given to the users;**

(Par [0155], lines 4-13, "**the user**, regardless of where it is **stored and in what format**. ... **the cookie is encrypted**.").

- **and a schema provider and user provider for providing an operation system independent of the authority information storing module,**

(Par [0278], lines 4-9, "Some of these attributes are part of structural object class, while others are part of auxiliary object classes (or auxiliary object class **schema**)...").

- **wherein the domain web server comprises an AA module for checking, by using the ACL cache, whether the user accesses;**

(Par [0352], "FIG. 46 shows a block diagram of two identity **servers that are equipped to communicate** with each other in ... function **modules** in set 1904. The following caches are representative of those in set 1906: (1) Access Control Policy Cache; (2) System Specific Data Cache; (3) Workflow Definition Cache; (4) X Structure Cache; (5) Server Information Cache; (6) **Application Information Cache**; and (7) Master Audit Policy Cache.").

- **an ACL cache which is delivered from the AA server;**

(Par [0106], " Access Server 34 provides authentication, authorization, auditing logging services. ... Servers.").

- **a decryption module for decrypting the encrypted AA cookies; and a module for processing a resource request from the user web browser,**

(Par [0380], lines 5-8, "In another implementation, the user **encrypts** the request using a private key and certificate registration **module 2072 is able to decrypt...**") and (Par [0433], lines 2-4, "requested resource is protected. In step 2630, **Web Gate 28 determines whether an entry for the requested resource is found in a resource cache**. ...").

- **wherein the domain web server checks the user authority by using ACL information, respectively, and produces the encrypted Role information cookie,**

(Par [0430], lines 10-16, "If the user has previously authenticated for a protected resource in the same domain, a valid authentication cookie is passed by browser 12 with the request in step 2550. The authentication cookie is intercepted by Web Gate in step 2552. If a valid cookie is received (step 2554), the method attempts to authorize the user in step 2556.").

- **this cookie signal being authenticated in the AA server 300, and, after authentication, Role, ACL, and ACE information is stored in the authority information storing module.**

(Par [0106], "**The Access System includes Access Server** 34, Web Gate 28, and Directory Server 36. Access Server 34 provides **authentication, authorization**, auditing logging services...Web Servers.") and (Col. [0097], lines 13-17, "The system decentralizes their administration by hierarchy delegating administrative **roles**.") and (Par [0381] Certificate registration **module** 2072 forwards the automatic renewal ... to **Certificate Authority** 2084 as a certificate signing request (step 2222). Certificate Authority...Certificate registration module 2072 updates the certificate in the data store...") and (Par [0107], lines 5-10, "The data elements of **the identity profile are called attributes**, ... The Identity Server includes three main applications, which effectively handle the identity **profiles and privileges of the user** population...") and

(Par [0143], "Examples ...of attributes stored in a group identity profile include: owner, name, description, static members, dynamic member rule, subscription policies, etc. Examples of **attributes stored** in a user organization identity profile include: owner, name, description, business category, address, country, etc. In other embodiments, less or more than the above-listed information is stored") and (Fig. 14, "provide list of proxies") and (Par [0177], "A **list of identified users** is then depicted on the substitute rights tab") "ACE" being all the "attributes stored".

As per Claim 2, the rejection of Claim 1 is incorporated and further Teng discloses:

> **- A method of managing access for an extranet, performed in the apparatus which comprises the elements in claim 1, the method comprising the steps of: a user web browser accessing a domain web server, an AA module of the domain web server confirming access authority of the user web browser,**

(Par [0398], lines 1-12 "If a status check is not required, **Identity Server** 40 exports the requested certificate to the user **via Web Server 20** (step 3434). ... Certificate Authority 2084, as described above with reference to FIG. 59A. In some embodiments, Identity Server 40 also **stores** the retrieved real time certificate status and related **validation information**") and (Par [0161], lines 5-7, "**Attribute access control** includes controlling who has view and modify permissions for each attribute.") and (Par [0113], lines 1-8, "With **Group Manager 44, companies** (or other entities) can allow **individual users to do the following**: ... **access to the applications** they need. Multi-step workflows can

then define which users must obtain **approval** before being added to a group and which can be added instantly.").

- **the user web browser requesting the authentication from the AA module of the AA server, the AA module of the AA server referring a schema provider to the authority,**

(Par [0109], lines 16-19, "An administrator can be delegated any allowed degree of responsibility. For example, a company might decide that only IT staff can assign **application access**") and (Par [0161], lines 1-7, "Configure tab 416 allows a user to configure various options for **User Manger 42**. The user must have sufficient privileges to access Configure tab 416. The user can perform attribute **access control**, delegate administration, define workflows and set the search base. **Attribute access control** includes controlling who has view and modify permissions for each attribute.") and (Par [0278], lines 4-9, "Some of these attributes are part of structural object class, while others are part of auxiliary object classes (or auxiliary object class **schema**)...").

- **the schema provider referring an authority information storing module to a site and delivering the referred result to a user provider,**

(Par [0233], "... **storing** a list of the groups in a file, **providing identifications of the groups** to another process, etc. In one example, **the access system** requests that the Identity System determine a user's groups so **that the access system can authorize a user to access** a resource based on membership in a particular group.").

- **and the user provider referring the authority information storing module to the user authority to make authentication and set user authority, and transmitting the information to the user web browser.**

(Par [0106], lines 1-8, "The Access System includes Access Server 34, Web Gate 28, and Directory Server 36. Access Server 34 provides **authentication, authorization,** auditing logging services. It further provides for identity profiles to be used across multiple domains and Web Servers from a single web-based authentication (sign-on). Web Gate 28 acts as an interface between Web Server 18 and Access Server 34.") and (Par [0478], lines 16-24, "In one embodiment, **Web Gate** 28 **transmits** a flag with all POST requests forwarded to Access Server...").

As per Claim 3, the rejection of Claim 2 is incorporated and further Teng discloses:

- **further comprising a user authority changing step comprising:**

(Par [0186], lines 4-5, "**changing attributes and working with certificates**.") "the attributes" including "authority".

if the user web browser requests the service enlisting or quitting, the resource request processing module of the domain web server requesting the AA module of the AA server to enlisting/quitting,

(Abstract, "...system identifies which workflows perform a requested task and are associated with a domain that includes the target of the task.") and (Par [0173], lines 12-22, "The **Master Access Administrator can configure a web gate**, configure an

access server, ... There can also be a delegated admin who can create/delete users, **add/remove users to/from groups, process workflow step**s, etc.").

- **the AA module changing the user authority information and sending the information to the user provider,**

(Par [0186], lines 4-15, "**changing attributes** and working with certificates. The template provides parameters that define how workflows can be created. Templates can be edited in order to tailor the workflow definition processes. The **User Manager...**").

- **the user provider updating the user information by sending the changed information to the authority information storing module,**

(Par [0109], "Multi-level delegation features also simplify individual user management. Companies ...modify personal or professional **information** ... (both inside and outside the company) ... (3) **change the information about users to grant or revoke services**. An administrator can be delegated any allowed degree of responsibility. For example, a company might decide that only IT staff can assign application access, whereas department managers can add new users.").

- **the AA module reporting to the resource request processing module that the user information was changed, such that the user is informed that the enlisting/quitting process is completed.**

(Par [0376], "Certificate Processing Server 2076 forwards the certificate to certificate registration module 2072 (step 2170). Certificate **registration module** 2072 stores the new certificate in certificate data store location 2082 (step 2156). Certificate registration module 2072 then **notifies the user that the certificate is in place** (step 2158).") and

(Par [0139], lines 21-29, "Note that when the access to the data stores includes a read operation, the **reporting of results** ... reporting a successful result of the write operation.").

As per Claim 4, the rejection of Claim 2 is incorporated and further Teng discloses:

- **an ACL initialization step comprising: the AA module of the domain web server requesting the ACL cache control module of the AA server to the ACL cache;**

(Par [0166], lines 1-6, "Configure tab 450 allows the entity to perform attribute access control, delegate administration, define workflows and define container limits. Attribute access control includes controlling who has view and modify permissions for each attribute of an organizational identity profile.") and (Par [0343], lines 5-7, "Therefore, Identity Server 40 provides each active request with a cache to reduce the number of data store accesses.").

- **and the ACL cache control module referring the ACL cache from the authority information storing module and delivering the referred data to the AA module of the domain web server,**

(Par [0344], "Each request is assigned to a thread of operation. Each thread has access to a small amount of memory in Identity Server 40 that is referred to as thread local storage. FIG. 44 provides an illustration of thread 1826, which resides in Identity Server 40 and contains thread local storage 1827. In accordance with the invention, thread local storage 1827 contains cache pointer 1828, which points to cache object 1829.

Cache object 1829 is reserved for caching data from entries in Directory Server 36 that are accessed by the request assigned to thread 1826.").

- **and an ACL synchronization step comprising: a supervisor instructing the ACL cache control module of the AA server to change the authority;**

(Par [0493], Access Server 34 evaluates whether the distinguished name of the authenticated user matches the distinguished name(s) called for by the **authorization rule**") and (Par [0405] The discussions above regarding workflows, groups, communication between Identity Servers, etc., primarily pertain to managing and using the Identity System. As stated above, the Identity System **manages identity profiles**. These identity profiles are used, among other things, to authenticate users and to authorize users to access resources. ...").

- **and the ACL cache control module requesting the authority information storing module to ACL change and the ACL cache of the domain web server to cache synchronization.**

(Par [0106], "**The Access System includes Access Server** 34, Web Gate 28, and Directory Server 36. Access Server 34 provides **authentication, authorization**, auditing logging services...Web Servers.") and (Par [0475], "...Access Server 34 retrieves the policy information from a policy domain cache, which cache's data from the directory server. The policy information can include one or more of the following: a URL absolute path, a query string, and zero or more query variables. In step 2741, Access Server 34 determines whether the **requested resource matches the policy resource**

type. If the resource type does not match, Access Server 34 skips to step 2752. ...") "matches" being the "synchronization" as claimed.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Angelica Ruiz whose telephone number is (571) 270-3158. The examiner can normally be reached on 7:30 a.m. to 5:00 p.m., ET.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Mohammad Ali can be reached on (571) 272-4105. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AR

MOHAMMAD ALI
SUPERVISORY PATENT EXAMINER